Privacy in MobilityFirst Architecture

Janne Lindqvist and Marco Gruteser
WINLAB, Rutgers University
Facebook tracking prompts call for FTC probe

Lawmakers say Facebook user tracking 'raises serious privacy concerns'

By Sharon Gaudin
September 29, 2011 04:01 PM ET

Computerworld - Facebook’s tracking technology has landed the social network in hot water, with two lawmakers calling for a Federal Trade Commission investigation of the social networking company.

Rep. Ed Markey (D-Mass.) and Rep. Joe Barton (R-Texas) wrote an open letter Wednesday urging FTC Chairman Jon Leibowitz to look into Facebook's tracking of its users even after they log out of the site.

The issue came to light just days after an Australian blogger published data showing that Facebook is gathering information on the online activities of its users.
Privacy Stakeholders

- **Users**
- Operators
- Network Providers
- Third-Party Service Providers
- Governments
- Intelligence Agencies
- Law Enforcement
- ...
- Several approaches to privacy, in this presentation focus
  - on user privacy, and
  - on possible technical solutions
Attacks Against User Privacy

• Who you are?
  – Have I seen you before?

• Who do you talk to?
  – Did you talk to them before?

• What are you talking about?

• What is your location?
  – Have you been here before?

• Note that these questions are connected
  – knowing places you go can tell who you are
  – e.g. home/work pairs have been shown highly likely to be unique
Attacker’s Location?

User → Access Point → Internet → Destination Server
Attacks Today: IP Packets

• can observe
  – Source and Destination IP addresses in all attack locations
  – Resolve and observe names

• You can change your source address, but research has shown that the set of your Destination IP addresses are highly likely to be unique

WINLAB
Amazon
Some blog
NSF
Attacks Today: IP Packets

• can observe
  – Source and Destination IP addresses in all attack locations
  – Resolve or observe names of destination

• might be interested in who is accessing particular server

Sees what is the source address

Some blog
Today: Solution Tor overlay
MobilityFirst: GUID and NA

- You can observe
  - Source and Destination GUID in all attack locations

- You can change your source address, but research has shown that the set of your Destination IPs are highly likely to be unique, same principle applies to GUIDs
MobilityFirst: GUID, NA at destination

- can observe
  - Source and Destination GUIDs in all attack locations
  - Resolve or observe names of destination

- might be interested in who is accessing particular server

Sees the source GUID, return packet “source” NA

Some blog
MobilityFirst Solution: Disposable Identifiers

- Disposable identifiers have been proposed several times [e.g. Gruteser’03, Lindqvist’05, Lindqvist’08]
- Today, even your disposable identifier is still often tied to your geographic location.
  - Thus, can discover where the packets are coming from

- In MobilityFirst, disposable identifiers do not have geographic or semantic mapping
  - (Unless we add these)
MobilityFirst Challenge: Reachability

- You can observe
  - Source and Destination GUIDs at all attack locations
  - Resolve or observe names of destination

- You can change your source address, but research has shown that the set of your Destination addresses are highly likely to be unique

GUID A → GUID B
GUID A ← GUID C
GUID A ← GUID D
GUID A ← GUID E
Conclusion

• Baseline privacy analysis

Ongoing work:
• Analysis on impact of disposable identifiers in MF
  – Today, routing scales because you can request only as many disposable identifiers (IP address) as have been provisioned to the network
  – In MF, you could have arbitrary number of disposable identifiers
• Reachability vs. Privacy
• Privacy by Default, what is the right level of privacy the network should provide?
Thank you